Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System

JYRI RAJAMÄKI, JARI AHOKAS & PARESH RATHOD
LaureaSID
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 ESPOO
FINLAND
jyri.rajamaki@laurea.fi, jari@jariahokas.fi, paresh.rathod@laurea.fi http://laureasid.com

Abstract: - Uninterrupted electric power supply and delivery is a part of Critical Infrastructure (CI) for modern society. Secure data transfer between the control center and power station is an essential requirement for controlling and protecting a power distribution system. Supervisory Control and Data Acquisition (SCADA) systems are at the core of power stations control infrastructure. Traditionally, SCADA systems use a proprietary communication network to transfer control signals. These signals are critical between central control systems and power stations. Current telecommunication networks used for the SCADA system do not provide the required capacity for modern Critical Infrastructure Protection (CIP) systems, such as real-time video streaming. In addition, present communication networks or internetworks do not give the required reliability and security for SCADA system. 'Multi-Agency Cooperation in Cross-border Operations (MACICO)' is an International Celtic Plus project to create an innovative communication model. The proposed model will combine multiple telecommunication networks including satellite, TETRA and 4G LTE. This innovative system will also support legacy and future communication technology like 2G, 3G. The MACICO project also includes subprojects. One is to create a secure, redundant and broadband data transfer channel for SCADA and video surveillance systems. This paper aims to propose a new model to address related problems. A proposed communication model relies on the Distributed Systems intercommunication Protocol (DSiP). DSiP allows the combining of various telecommunication resources into a uniform and easy maintain system. The paper is also comparing available solutions of the research problem.

Key-Words: - SCADA, Critical Communications, Secure Communications, Distributed Systems intercommunication Protocol, DSiP, MACICO, Cross-Border Operations, Multichannel networks

1 Introduction

Multi Agency Cooperation in Cross-Border Operations (MACICO) is an international Celtic-Plus research project. The project is aiming to develop a concept for interworking of critical infrastructure protection and public safety organizations in their daily activities. "MACICO's main purpose is addressing in a short-term stand needs for improved systems, tools and resources for radio broadcasting in cross-border operations as well as during operations taking place on the territory of other member states. Study shows high scale civil crisis operations or complex emergencies needing support of Public Safety Services from other Member States", [1]. On the other hand, MACICO also encompasses the interoperability issues European countries can experience in a long-term perspective, tackling the necessary conversion between currently deployed legacy system and future broadband networks [1].

Recent research indicates the importance of video surveillance system in the Critical Infrastructure Protection (CPI). In addition, perimeter monitoring is enhancing security [2], [3]. Live video streaming from prime locations of power stations becoming more prominent because of security threats to the system.

Currently electricity distributing companies are using proprietary communication channels along with conventional public Internet connections. It is clear that the current standard Internet connection, such as ADSL is struggling to provide Quality of Service (QoS). The research case is a power company in the Southern Finland region where experiments carried out. The company is using a standard commercial grade ADSL connection with VPN tunneling devices for SCADA communication

and video surveillance since last four years. However, the largest drawback was certain limitations regarding mission critical usage. Further, our study is showing that data transfer including the video stream from the power station requires secure and reliable connections to the command and control rooms.

This paper introduces a new way of approaching this problem by combining two previously separate data transfer systems. The more fault resistant system is achieved by connecting these independent channels together with added functionality without adding any complexity to the application layer.

2 Study Domain and Applicable Technologies

This section introduces detailed information on research domain and relevant technologies. Mainly, SCADA and surveillance systems and their requirements for data transfer systems.

2.1 SCADA Systems

SCADA refers to the industry control and monitoring systems including infrastructure, facility, productions or manufacturing processes. SCADA systems are used for supply, control and monitoring daily necessity for modern society. "SCADA protocols consist of Conitel, Profibus, Modbus RTU and RP-570. Standard protocols are mainly IEC 61850, DNP3 and IEC 60870-5-101 or 104" [4], [5]. These protocols are standardized and operated over Transmission Control Protocol / Internet Protocol (TCP/IP).

The SCADA system collects and transmits field data to master stations via Remote Terminal Units (RTU). Timely and accurate data are critical to conduct efficient, reliable and secure operations. Broadly there are two types of SCADA software, proprietary and open [6].

2.2 Access Control and Surveillance System

Access control and video surveillance are the most useful tools for various assets to protect against deliberate or accidental damage or theft. In addition, on various occasions existing vulnerabilities can be overcome by these tools.

Contactless access control could be implemented, which enables the UHF RFID technology. RFID (Radio Frequency Identification) is a general term for technologies operating in the radio frequencies used for identification. Technology is relying on information storage, an RFID tag, and its wireless reading using radio waves. In practice, the use of RFID technology brings benefits and resolves current problem that a traveling movement of tag to be identified automatically [7].

2.3 Video Surveillance System

Nowadays, video surveillance systems are useful for purposes like space missions and border frontier guard. Video surveillance is often a hideous task for an operator to monitor at the command and control center. This task is easier to execute with the application of technical solutions where less human interaction needed on the monitoring process [8].

2.4 Communication Systems Operating in Sparsely Populated Area

Normally power stations are sparsely located from resident area. Different data transfer network systems including leased line connections to commercial mobile networks, satellite and TETRA (Terrestrial Trunked Radio) networks are used to transfer data from sparsely populated areas.

Other technology like GSM was initially design as a pan-European mobile communication network. "General Package Radio Service (GPRS) is enabling an improved data transfer rate performance by allowing for more than one GSM timeslot to be used by a terminal for a service at a time [2]". The driving factor for new (and higher bandwidth) data service obviously is wireless access to the Internet [2], [9].

The Third-Generation (3G) mobile communication networks known as the Universal Mobile Telecommunications System (UMTS) in Europe and across the world [2]. However, the 2G networks are close to their end of life cycle. The 3GPP Long-Term Evolution (LTE) is aiming to be a mobile communication system that can take the telecom industry in to the 2020s [10].

"TETRA is an open digital radio standard for professional mobile radio [11]". TETRA is more useful communicating with the mobile and remote work force along with commercial usage. Public safety and emergency service providers including police and fire departments are the most essential group of users of TETRA [11].

Often, the satellite refers as an "orbit radio star" for reasons that can be easily appreciated. A communication satellite is a repeater station that receives signals from ground, processes them and then retransmits them back to the Earth [12].

ISBN: 978-960-474-336-0

Power Line Communications (PLC) is widely accepted and easily deployed method for communication with power stations. The live video streaming can be achieved depending on frequencies and modulation techniques within available speeds [13]. PLC is also suitable solution for SCADA communications. However, it would not be suitable as only communications channel for mission critical systems.

3 Research Problem and Methodology

Our research and experiment case is focusing on the power grid application and their infrastructure protection. The existing solutions and services are lacking some substantial feature to provide Quality of Service for Critical Infrastructure Protection (CIP) and SCADA systems. These challenges lead us to form research questions and find their solutions. How to provide secure and reliable communications to CIP and SCADA systems?

Computer science technical solutions are facing challenges of current business problem. If we put innovative artifacts into the action and analyze how they are used and how they performed, we will see things that cannot be seen in the laboratory [14]. Management information systems (MIS) involve three primary resources: people, technology, and information. The MACICO project follows the basic development research in the MIS wheel diagram, first published in 1991 [15]. According to the "going the last mile" approach [14], the starting point of research should be a real problem for real people. In this project, real problem came from governmental SCADA systems and CIP in Finland who are experiencing challenges. This project integrated science both in the laboratory and the field (see Fig. 1).

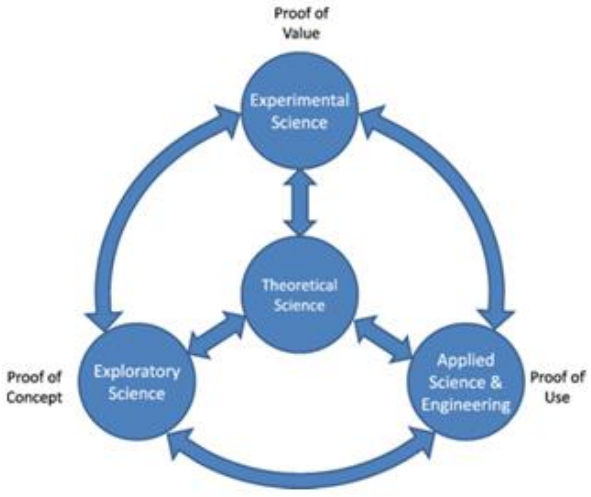

Fig. 1 Integrated multi-disciplinary and methodological development research

4 Proposed System

The communication solution should be flexible and adoptable to any changes caused by data transport layers. For example, management of services is based on available data channel bandwidth. Another significant characteristic and functionality requirement is maintaining the priority of message transport. Hence, site surveillance and SCADA-command and control should be carefully contemplated before implementation.

The proposed solution is utilizing multichannel communications resources spreading across the control room to the power station. It will perform SCADA-command and control messaging with the broad range of surveillance and monitoring systems including CCTV. The solution is aiming to provide consistent communication system considering requirements of smart-grid system, command and control of electrical substation; as well as site surveillance and perimeter monitoring.

4.1 Multichannel Communication

MACICO and related projects (for example, Mobile Object Bus Interaction - MOBI) are experimenting and studying multichannel communication. There are promising results, and some are noteworthy to mention here. A multichannel data communication method supplies a way to communicate over virtually any type of telecommunications media in such a way that parallel paths appear as a single robust, uninterruptable, secure and reliable communication link between communicating peers [16]. The solution is based on DSiP (Distributed Systems intercommunication Protocol). It is making possible to interoperate and flawless data transfers amongst various service providers, resulting in a true multichannel communication system. DSiP increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems [16.] This is achieved by (1) splitting risks between operators and communication channels, (2) better routing and priority capabilities that takes security and intrusion risks into account and (3) adding modularity [3], [17].

The USA Office of Emergency Communications is aiming for Nationwide Public Safety Broadband Network, FirstNet, to be based on LTE network technology [18]. LTE networks are vulnerable to the wireless interface jamming using low cost relatively simple devices as described in Virginia Tech preliminary research [19]. If networks build on LTE

ISBN: 978-960-474-336-0

technology were to be compromised, existing 2G and 3G networks would still operate without problems. However, those older networks are gradually being phased out.

Combining different forms of communication networks is a challenging task. The DSiP solution integrates the quality of service definitions for a variety of traffic. Traffic priority levels can be based on the destination of the IP traffic flow in question or by analyzing the TCP headers. By using DSiP, it can be safer assumed that any User Datagram Protocol (UDP) traffic is neither time sensitive nor needing a highly reliable communications channel. It is also possible to divide, and direct traffic flows to a different channel based on the routing costs of each channel. All these features are combined in to a single device. DSiP solutions classify traffic flow and take routing decisions based on the priority of individual traffic channel and flow.

4.2 Built in Security

The requirement for secure communications in SCADA networks have been studied earlier, and the proposed DSiP system fulfills identified reliability and security feature requirements [20]. As the earlier paper states, there are also other security and high availability features that have to be considered such as fault tolerant network switches or uninterrupted power supply for network appliances. Fig. 2 shows an example of Closed-circuit television (CCTV) and SCADA communications combined it a single communications framework.

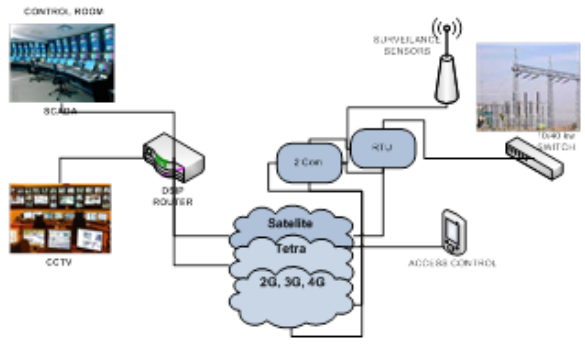

Fig. 2 Secure Communications for Electricity Supply Deployment

DSiP infrastructure has powerful built in security measures for securing critical infrastructure communications, such as power stations. Several key factors for strong security are included in the DSiP. These elements are usage of IPsec protocol, encryption based on secure ciphers such as Advanced Encryption Standard AES-256, packet time stamping, sophisticated firewall and prevention of denial of service (DoS) attacks. Deploying DSiP system can help in achieving North America Electric Reliability Corporation (NERC) standards, especially targeted for CIP. NERC CIP 002-009 documents set demanding reliability and security standards for protecting SCADA communications [21].

Combining two fundamentally different communications requirements can be achieved with the DSiP system. Video surveillance data requires high-bandwidth. It can survive network packet loss without functionality loss while SCADA commands require reliability and relatively sparse network delay. The DSiP system separates these requirements from each other and delivers the required functionality to both use cases.

4.3 Test Setup

DSiP-based systems have been in operative use in critical installations for several years, for example, the Finnish Coast Guard's coastal surveillance solution and SCADA control of Finland's main power grid [22]. However, simultaneous transmission of data for applications with so diverse requirements and characteristics than SCADA and CCTV needs testing. Different kind of DSiP nodes and router has been tested at Laurea University of Applied Sciences (LUAS). The required DSiP routers and communications devices, such as satellite and 3G modems, have been installed, also, in a police vehicle for testing purposes as a part of Mobile Object Bus Interaction (MOBI) project. There will be a proof of concept vehicle as an outcome of MOBI project. Among other things, similar data communications solutions are under testing for SCADA control.

The MOBI demo vehicle is equipped with multichannel router that is simultaneously connected to satellite, TETRA, and 3G data networks. Data communications solution is evaluated by field tests. [17]

5 Discussion

The DSiP device and software package can hide the complexity of the network architecture from the applications and especially from the end users. However, a problem with TCP network convergence still exists and needs to be examined in more detail.

ISBN: 978-960-474-336-0

5.1 TCP Protocol Challenges in Fluctuating Networks

TCP protocol has inherited problems with congestion protocols when switching to different network layers that use various techniques. Congestion protocol challenges are noticeable when delay or speed of the network link changes considerably in a situation like switching either from 2G to LTE network. The TCP protocol requires relatively long time to adjust to the new network environment after the vertical network handover.

Normally this would not harm SCADA connections since communication with devices is not bandwidth incentive. Short delays caused by TCP protocol readjusting itself should not cause difficulties for SCADA control, since commands are usually small and can even be fitted into a single TCP/IP encapsulated packet.

General TCP algorithms for vertical network handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in that the receiver reports to the sender that duplicate segment has been received. The Eifel detection provides a faster detection of Spurious Retransmission Timeouts (RTO) compared to DSACK. Forward RTO-Recovery is a TCP sender-only implemented algorithm that helps to detect Spurious RTOs. It does not require any additional TCP header options to operate. TCP congestion control algorithms have been designed to enable TCP to adapt to the fluctuating bandwidth available on its end-to-end path. TCP connection remains fairly stable over the lifetime of a connection.

Proposed enhancements are implemented in the TCP SACK algorithm. These are invoked when a cross-layer notification arrives from the mobile node to the TCP sender. This information contains occurrences of a handoff and rough estimates of the bandwidth, also delay of the old and the new access links.

In the absence of the cross-layer information, the proposed enhancement does not affect the normal behavior of the TCP algorithm [23]. A modified backpressure routing algorithm can separate the two time scales of Intermittently Connected Networks (ICN). It is presented in Jung Ryu's research; this algorithm improves performance. On top of this, algorithm is a rate control protocol implemented on TCP protocol [24].

5.2 Alternatives for the SCADA Communications

There are other alternatives to the DSiP solution. One solution would be crossed crypto-scheme integration to the SCADA system in Smart Grid environment [25]. This solves the problem of securing the communication channels, but does not tackle the problem of managing several communications channels in an effective manner. However, using only the said solution does not answer the question of how to deliver several reliable communications channels seamlessly to the application layer, SCADA in this use case. The application itself should not be required to manage all possible communication channels combinations in the grid.

In case of power stations, usages for ad hoc communications methods are few. One solution for managing communication paths using ad hoc networks is the Ad hoc On-Demand Distance Vector (AODV) algorithm [26]. There are situations where all connections to the backbone network are entirely lost. In such situations, theoretically it would be possible to transfer data from the affected area. ICN is this kind of technique.

5.3 Quality of Service (QoS)

For communications to be successful, it is also essential to focus on network traffic prioritizes for different types of communication streams. A different technique required for assuring high-transport priorities while operating without DSiP systems. To solve this issue, a suitable QoS mechanism must be utilized. It is worth noting that many available commercial communications networks do not honor QoS tags in IP traffic.

5.4 Comparison of Available Solutions

The proposed DSiP solution has several advantages compared to other technologies. Table I presents a comparison between the solutions introduced in this paper. The DSiP system does not require applications to be aware of any of the communications routes and/or the characteristics of the underlying networks.

The table lists different technical solutions described in previous chapters. Features of the solutions are compared, and as a result, DSiP has the most beneficial feature set amongst them. There is one thing that not directly addressed by DSiP being TCP protocol issues in vertical network handovers. However, it must be noted that none of

the compared technology offers a consolidated result for fluctuating TCP networks. However, further research work is recommended for a complete end-to-end solution.

Table 1 Comparison of Technical Solutions

	DSiP	DiffServ	Crossed Crypto-Scheme	Ad hoc networks	ICN
Multiple network routes	x	x	x	x (many point-to-point connections)	x
QoS	x	x			
Single device / hardware solution	x				
TCP enhancements in fluctuating networks					x
Built in security features	x		x	x (if network permits)	
Cost control based on network route	x		x (static)		

5.5 Integrating Existing Systems to the DSiP

All communications should be carried over IP-protocol in order to DSiP solution to function. For power stations, this sets a requirement of using devices converting traditional serial port based traffic to IP based traffic. Existing equipment can be converted to IP traffic by using a serial to IP converter or a RS-232 to Ethernet by other name. Installing new natively IP enabled equipment, replacing older RS-232 devices might not be economically viable solution since SCADA systems can have a pretty long life span.

6 Conclusion

The Critical infrastructure is composing electricity generations, transmissions and distributions. That is essential for the functioning of a 21st century society and economy. SCADA systems are used for controlling the electric power stations. SCADA systems require high reliability and they may have very strict requirements on low latency. For added electrical power station security, a broad range of surveillance systems are needed, video surveillance being crucial. Current telecommunication networks used for SCADA systems do not support major volumes of information to be conveyed for real time video.

The MACICO (Multi-Agency Cooperation In Cross-border Operations) project is aiming to resolve this problem interconnecting different telecommunication networks and combining various communications ways in a single logical communications channel. An objective is to create a redundant, secure and fast single data transfer system for SCADA and video surveillance. The data transfer system should have the performance and capabilities needed to handle these diverse requirements and characteristics in an efficient way. The DSiP can solve many of the challenges with communications over different networks in a single solution

A more fundamental problem with the TCP protocol itself needs to be address. This could be resolved with a help from the DSiP router in a form of providing information about the underlying network layer features. Further studies and research need to carry out on IPv6 networks with DSiP.

DSiP solution is likely to be more expensive compared to a single channel communications. The cost increases because of the need for specific communications networks, and more intelligent communications equipment and software. New and improved communications solution can diminish the power outage affecting thousands of users or even completely inhibit the outage from occurring in the first place. The cost savings would be enormous when compared to the initial investment costs.

One possible solution to develop critical infrastructure reliability is systems architecture based on cloud computing. This project also contributes producing a solution useable across borders in several countries. The international power companies operating in different countries are examples of cross border users for DSiP solution.

References:

[1] *MACICO project information*, http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

[2] J. Eberspächer, H. J. Vögel, C. Bettstetter and S. Hartmann, *GSM architecture protocol and services*, Third Edition. John Wiley & Sons Lt.d Great Britain. 2011.

[3] J. Holmstrom, J. Rajamaki and T. Hult, The Future Solutions and Technologies of Public

Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication, *International Journal of Communications*, Issue 3, Volume 5, 2011.

[4] A. Daneels and W. Salter, What is SCADA? *International Conference on Accelerator and Large Experimental Physics Control Systems*, Trieste, Italy, 1999

[5] *SCADA*, http://www.scadasystems.net/, http://www.controlmicrosystems.com/resources-2/faqs/scada11/

[6] G. Clarke and D. Reynders, *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*, Elsewier, Great Britain, 15-16, 19, 163, 2004.

[7] UHF Wristband Sport. Retrieved October 5, 2012 from: http://www.rfidtag.cz/uhfwristbandsport.html.

[8] D. Kieran, J. Weir & W. Yan, A Framework For An Event Driven Video Surveillance System, *Journal of Multimedia*, Volume 6, Number 1, February, 3-13, 2011.

[9] J. Korhonen, *Introduction to 3G Mobile Communications*, Second Edition. Artech House. Norwood, MA. 3, 14, 2003.

[10] E. Dahlman, S. Parkval, J. Sköld and P. Beming, *3G Evolution: HSP and LTE for mobile Broadband*, Second Edition. Academic Press. Burlington, MA, 9, 22, 2008.

[11] P. Stavroulakis, *Signals and communication technology, Terrestrial Trunked Radio-TETRA, A Global Security Tool*, Springer, Heidelberg, 2, 27, 51, 170, 2007.

[12] A. Maini and V. Agrawal, *Satellite Technology: Principles and Applications*, John Willey & Sons Ltd, Noida, India, 4, 2011.

[13] H. C. Ferreira, L. Lampe, J. Newbury and T. G. Swart, *Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines*, John Wiley & Sons, United Kingdom, 2010.

[14] R. Winter, Interview with Jay F. Nunamaker, Jr. on "Toward a Broader Vision of IS Research", *Business & Information Systems Engineering*, Vol. 2: Iss. 5, 321-329, 2010.

[15] J. F. Nunamaker, Jr., M. Chen and T. D. M. Purdin, Systems development in information systems research, *J. Manage. Inf. Syst*. 7, 3, 89-106, 1990.

[16] J. Ahokas, J. Rajamäki and I. Tikanmäki, Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations, *International Journal of Communications*, Issue 1, Volume 6, 2012, 120-127, 2012.

[17] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, *Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux* (SCVT), Nov 24-25, 2010. *Vehicular Technology in the Benelux (SCVT)*, Nov 24-25, 2010.

[18] Office of Emergency Communications, *Nationwide Public Safety Broadband Network*, USA, 2012 Retrieved April 22, 2013 from The U.S. Department of Homeland Security (DHS), http://www.dhs.gov/sites/default/files/publications/FactSheet_Nationwide PublicSafetyBroadbandNetwork.pdf

[19] Wireless @ Virginia Tech, *A brief response to the FirstNet NOI regarding the conceptual network architecture*, USA, 2012 Retrieved April 22, 2013 from Wireless@ Virginia Tech http://www.ntia.doc.gov/files/ntia/va_tech_response.pdf

[20] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence and M. Pozzuoli, "Securing SCADA Communications following NERC CIP Requirements", *Asia Energy Week 2008*, Kuala Lumpur, Malaysia, May, 2008.

[21] *NERC Standard CIP-002-3 through -009-4, Cyber Security*, 2009-2012 Retrieved November 10, 2012, from North American Electric Reliability Council (NERC), Critical Infrastructure

[22] J. Rajamäki, The MOBI project: Designing the future emergency service vehicle, *IEEE Vehicular Technology Magazine*, June 2013 [In Press].

[23] L. Daniela, Cross-layer Assisted TCP Algorithms for Vertical Handoff, *Department of Computer Science Series of Publications Report* A-2010-6, University of Helsinki Finland, 2010.

[24] J. Ryu, *Congestion Control and Routing over Challenged Networks*, The University of Texas at Austin, 2011.

[25] R. Robles and T. Kim, Communication Security for SCADA in Smart Grid Environment, *WSEAS Conference in Advances in Data Networks, Communications, Computers*, 2010.

[26] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung and Y. Lee, Development of Ad hoc Network for Emergency Communication Service in Disaster Areas, *Proceedings of the 9th WSEAS International Conference on Applications of Computer Engineering*, 2010.